

METHOD AND SYSTEM FOR DIGITAL IMAGE AUTHENTICATION

ABSTRACT OF THE DISCLOSURE

5 A digital image (27) is taken by a digital camera  
(12) and a serial number (22) is associated with the  
digital image. The digital image is encrypted by the  
camera using a camera key (20) to form an encrypted  
image (28). The encrypted image is then communicated to  
10 an authentication center (14). The authentication center  
associates the encrypted image with the serial number  
identifying the camera and an encrypted camera key (50).  
At a later time, a digital image is sent by a verifying  
entity (16) to the authorization center to determine if  
15 the digital image has been altered. The authorization  
center then decrypts the encrypted image, compares the  
digital image to the decrypted encrypted image and  
reports the result to the verifying entity. Also, the  
digital image is encrypted. The digital image is  
20 partitioned into at least one partition. A P box is  
applied to each partition. A first and second S box are  
applied to each partition. The encrypted image is  
generated based the P box, the first S box and the second  
S box. The authentication center decrypts the digital  
25 image. The encrypted digital image is decrypted by  
determining at least one partition based on the encrypted  
digital image. At least one trajectory associated with  
the encrypted image is reconstructed. A reverse S2 box,  
a reverse S1 box and a reverse P box are applied to the  
partitions. The original digital image is generated  
30 based on the first reverse S box, the second reverse S  
box and the reverse P box.